AMENDMENT TO THE CLAIMS

Claims 1-9, 12, 14, 16-17, 20, 22-32, 35-36, 44-66 remain in this application. Claims 1, 23, 50, 57, and 62 have been amended. Claims 32, 34, and 37-43 have been canceled. No new claims have been added.

*Listing of Claims:*

1. (Currently Amended) A system, comprising:

a local area network (LAN) having at least one host device, the at least one host device having software to perform anti-virus scanning;

a communication module to communicate anti-virus protection information for the at least one host device to an access module, the anti-virus protection information including status of anti-virus protection of the at least one host device; and

the access module coupled to the LAN to maintain a policy regarding anti-virus protection for the LAN and manage anti-virus protection scanning performed by the at least one host device, the access module to exchange anti-virus protection information with the at least one host device using the communication module of the at least one host device, and, ~~and to deny the at least one host device access to the Internet~~ if the status of the anti-virus protection of the at least one host device is not compliant with the policy, to deny the at least one host device access to the Internet and to bring the anti-virus protection of the at least one host device into compliance with the policy.

2. (Original) The system defined in Claim 1 wherein the communication module is part of the at least one host device.

3. (Original) The system defined in Claim 1 wherein the access module sends at least one command to the at least one host device via the communication module.

4. (Original) The system defined in Claim 3 wherein the at least one command comprises a command selected from a group comprising: a command to request status of the anti-virus protection of the at least on host device, a command to have the at least one host to update the anti-virus protection, a command to uninstall the anti-virus protection, and a command to check a specific file or directory.

5. (Original) The system of claim 1, wherein a system administrator sets a range of compliance for the anti-virus protection policy.

6. (Original) The system of claim 5, wherein the Internet access module denies access to the Internet to the at least one host device if not in the range of compliance.

7. (Original) The system of claim 1, wherein the access module enforces and maintains the anti-virus protection policies for more than one host device.

8. (Original) The system of claim 7, wherein the anti-virus protection policies differ between host devices on the LAN.

9. (Previously Presented) The system of claim 1, wherein the status of the anti-virus protection of the host device includes a version number of the anti-virus protection software on the host device.

10. (Canceled)

11. (Canceled)

12. (Previously Presented) The system of claim 1, wherein the status of the anti-virus protection of the host device includes a time stamp indicating when the anti-virus protection software was last updated on the host device.

13. (Canceled)

14. (Original) The system of claim 1, wherein the access module initiates an update in anti-virus protection for the host-device.

15. (Canceled)

16. (Original) The system of claim 1, wherein the host device reports a problem with a virus to the Internet access module.

17. (Previously Presented) The system of claim 1, wherein the access module is one or more of:

a live firewall, a proxy server, a router, or a gateway.

18. (Canceled)

19. (Canceled)

20. (Original) The system of claim 1, wherein the access module is a modem.

21. (Canceled)

22. (Original) The system of claim 1, wherein the access module is an application server.

23. (Currently Amended) A method, comprising:

connecting a local area network to an Internet via an Internet access module;

connecting a host device to the Internet via the local area network; and

using the Internet access module to enforce a policy for anti-virus protection on the host device based on the status of anti-virus protection on the host device, wherein the using includes,

denying the host device access to the Internet if the status of the anti-virus protection on the host device is not compliant with the policy[[.]], wherein the denying includes,

applying a range of compliance for the anti-virus protection policy set by a system administrator,

removing the range of compliance and requiring

the most current anti-virus protection upon notice of a virus alert.

24. (Previously Presented) The method of claim 23, further comprising connecting the host device with the Internet access module via an out of band protocol.

25. (Previously Presented) The method of claim 24, further comprising communicating a version number of the anti-virus protection on the host device to the Internet access module over the out of band protocol.

26. (Previously Presented) The method of claim 24, further comprising communicating a time stamp indicating when the anti-virus protection was last updated on the host device to the Internet access module over the out of band protocol.

27. (Previously Presented) The method of claim 24, further comprising initiating an update in anti-virus protection for the host-device over the out of band protocol.

28. (Previously Presented) The method of claim 24, further comprising encrypting the out of band protocol.

29. (Previously Presented) The method of claim 23, further comprising connecting more than one host device to the local area network.

30. (Previously Presented) The method of claim 29, further comprising using the Internet access module enforces and maintains the anti-virus protection policies for more than one host device.

31. (Previously Presented) The method of claim 30, wherein the anti-virus protection policies differ between host devices.

32. (Canceled)

33. (Canceled)

34. (Canceled)

35. (Previously Presented) The method of claim 23, further comprising the host device is checked repeatedly to make sure the anti-virus protection is not disabled.

36. (Previously Presented) The method of claim 23, further comprising reporting a problem with a virus to the Internet access module.

37. (Canceled)

38. (Canceled)

39. (Canceled)

40. (Canceled)

41. (Canceled)

42. (Canceled)

43. (Canceled)

44. (Previously Presented) A system, comprising:

a local area network (LAN) having at least one host device, the at least one host device having software to perform anti-virus scanning;

a communication module to communicate anti-virus protection information for the at least one host device to an access module, the anti-virus protection information including status of anti-virus protection of the host device; and

the access module coupled to the LAN to maintain a policy regarding anti-virus protection for the LAN and manage anti-virus protection scanning performed by the at least one host device, the access module to exchange anti-virus protection information with the at least one host device using the communication module of the at least host device and to deny the at least one host device access to the Internet if the at least one host device does not have anti-virus protection compliant with the policy, wherein compliance with the policy is either a range of compliance or the most up to date anti-virus protection depending on whether there is currently a virus alert.

45. (Previously Presented) The system of claim 44, wherein the access module enforces and maintains the anti-virus protection policies for more than one host device; and

wherein the anti-virus protection policies differ between host devices on the LAN.

46. (Previously Presented) The system of claim 44, wherein the status of the anti-virus protection of the at least one host device includes one or more of a version number of the anti-virus protection software on the host device and a time stamp indicating when the anti-virus protection software was last updated on the host device.

47. (Previously Presented) The system of claim 44, wherein the access module initiates an update in anti-virus protection for the at least one host device.

48. (Previously Presented) The system of claim 44, wherein the at least one host device reports a problem with a virus to the access module.

49. (Previously Presented) The system of claim 44, wherein the access module is one or more of:

a live firewall, a proxy server, a router, a modem, a gateway, or an application server.

50. (Currently Amended) An apparatus comprising:

an Internet access module to be coupled to connect the Internet and a local area network (LAN) including host devices, the Internet access module to receive from the

host devices their anti-virus protection status and to deny Internet access to those of the host devices whose anti-virus protection status is not compliant with a corresponding anti-virus protection policy and make available software components necessary to bring those host devices whose anti-virus protection status is not compliant into compliance with the corresponding anti-virus protection policy.

51. (Previously Presented) The apparatus of claim 50, wherein the anti-virus protection policy includes a range of compliance.

52. (Previously Presented) The apparatus of claim 50, wherein the anti-virus protection policy differs between the host devices on the LAN.

53. (Previously Presented) The system of claim 50, wherein the status of the anti-virus protection of at least one of the host devices includes one or more of a version number of the anti-virus protection software on that host device and a time stamp indicating when the anti-virus protection software was last updated on that host device.

54. (Previously Presented) The system of claim 50, wherein the Internet access module initiates an update in anti-virus protection for at least one of the host devices.

55. (Previously Presented) The system of claim 50, wherein the Internet access module is one or more of:

a live firewall, a proxy server, a router, a modem, a gateway, or an application server.

56. (Previously Presented) The system of claim 50, wherein compliance with the anti-virus protection policy is either a range of compliance or the most up to date anti-virus protection depending on whether there is currently a virus alert.

57. (Currently Amended) A method comprising:

enforcing anti-virus protection in a module providing Internet access to a plurality of host devices belonging to a local area network by performing the following for each of the plurality of host devices repeatedly,

receiving status of the anti-virus protection on the host device,

determining compliance with an anti-virus protection policy based on the anti-virus protection status, ~~and~~

denying Internet access to the host device if its anti-virus protection status is determined not compliant[[.]], and

providing software components to bring the host devices into compliance with the anti-virus protection policy if its anti-virus protection status is determined not compliant.

58. (Previously Presented) The method of claim 57, wherein the determining compliance including determining if the anti-virus protection status is within a range of compliance.

59. (Previously Presented) The method of claim 57, the performing for each of

the plurality of host devices also includes removing the range of compliance upon notices of a virus alert.

60. (Previously Presented) The method of claim 57, wherein status of the anti-virus protection includes one or more of a version number of the anti-virus protection software on the host device and when the anti-virus protection software was last updated.

61. (Previously Presented) The method of claim 57, wherein the performing for each of the plurality of host devices also includes initiating an update of the anti-virus protection on the host device.

62. (Currently Amended) A machine-readable medium that provides instructions, which when executed by a machine, cause said machine to perform operations comprising:

enforcing anti-virus protection in a module providing Internet access to a plurality of host devices belonging to a local area network by performing the following for each of the plurality of host devices repeatedly,

receiving status of the anti-virus protection on the host device,

determining compliance with an anti-virus protection policy based on the anti-virus protection status, ~~and~~

denying Internet access to the host device if its anti-virus protection status is determined not compliant[[.]]; and

providing software components to bring the host devices into compliance with the anti-virus protection policy if its anti-virus protection status is determined not compliant.

63. (Previously Presented) The machine-readable medium of claim 62, wherein the determining compliance including determining if the anti-virus protection status is within a range of compliance.

64. (Previously Presented) The machine-readable medium of claim 62, the performing for each of the plurality of host devices also includes removing the range of compliance upon notices of a virus alert.

65. (Previously Presented) The machine-readable medium of claim 62, wherein status of the anti-virus protection includes one or more of a version number of the anti-virus protection software on the host device and when the anti-virus protection software was last updated.

66. (Previously Presented) The machine-readable medium of claim 62, wherein the performing for each of the plurality of host devices also includes initiating an update of the anti-virus protection on the host device.